REPUBLIC OF CAMEROON

*************

*Peace work home*

*************

MINISTRY OF HIGHER EDUCATION

*************

COAST UNIVERSITY INSTITUTE

*************

*Institute of Computer Engineering of Central Africa*

*************

MASTER'S DEPARTMENT CS2I

*************

# AUTOMATIC DETECTION / PREVENTION OF INTRUSIONS USING SENSORS DISTRIBUTED IN A COMPUTER NETWORK. Case study: IP-TELRA

Written and presented by**:**

**TIOWA NZONTEU**

Registration number :

**ISTDI15E010728**

Under the direction of:

**Dr TEGUIA Jean Blaise**

**Mr. TEKEU Hypolith**

**Mr HAMENI Christian**

**Academic year: 2021-2022**

# Summary

# List of Figures

# List of paintings

# Introduction

Computer networks have become vital and deterministic resources for the proper functioning of companies. In addition, these networks are open in that they are mostly connected to the Internet.[1]. This openness, which facilitates communication, unfortunately creates significant risks in the field of computer security. Data recently published by the National ICT Agency (ANTIC) reveals financial losses of more than 12 billion FCFA in Cameroon due to cybercrime in 2021, twice as much as the year 2019[2]. Internet users are not necessarily full of good intentions, they can exploit the vulnerabilities of networks and systems to carry out their attacks. The consequences of these attacks can be serious for an individual (loss of information, or even worse the theft of information, breach of privacy, etc.) and for a company (loss of know-how, damage to the image brand, financial loss, etc.). For this, administrators deploy effective security solutions capable of protecting the company's network.

Reducing or eliminating security flaws in a network in order to reduce the risks of threats materializing has become an important point in setting up networks. Among the precepts known in the field of computer security, there is the one stating that for a company connected to the Internet, the problem today is no longer whether it will be attacked, but when it will happen.[3]; a possible solution is then to try to postpone the risks over time by implementing various means intended to increase the level of network security. It is therefore necessary to have specialized tools whose role will be to monitor the data passing through a system and to react if some of them seem suspicious. The software that is best able to perform this task are intrusion detection and prevention systems. When we arrived at the IP-TELRA company, this type of system did not exist, thus putting the company in a state of permanent vulnerability to attacks, although it has a minimum level of security but does not not guaranteeing the security of the data and entities of its internal network in the best possible way in view of the importance and criticality of these.[2][4]. The main objective that guides us in this work is to propose a distributed architecture for the detection and prevention of intrusions based on the use of intrusion detection systems. We also propose a network of honeypots whose purpose is to study the threats against IP-TELRA, in order each time to readapt the policy implemented in the detection systems against new threat trends. To succeed in our work we will have to, Install Bro IDS for packet filtering, Create filter rules to secure the network, Install a honeypot computer to deceive attackers, Communicate the different equipment in the network, Put set up a distributed IDS network. We propose in this project, a distributed architecture approach to detecting and preventing intrusions based on the use of an intrusion detection system. Also, we offer a space for studying attack mechanisms, based on honeypots. The combination of these two means will make it possible to offer a slightly more reliable surveillance environment to the IP-TELRA company network.

# study of the existing

The analysis of the existing makes it possible to understand the nature of the current system, describes the present solution of the field of study to the term of organization. The purpose of the analysis of the existing is to find the strengths and weaknesses of the existing system. Thus, the analysis of the existing makes the inventory of fixtures of the current system.

## Presentation of the existing network architecture

The existing network architecture to date at IP-TELRA is as follows:

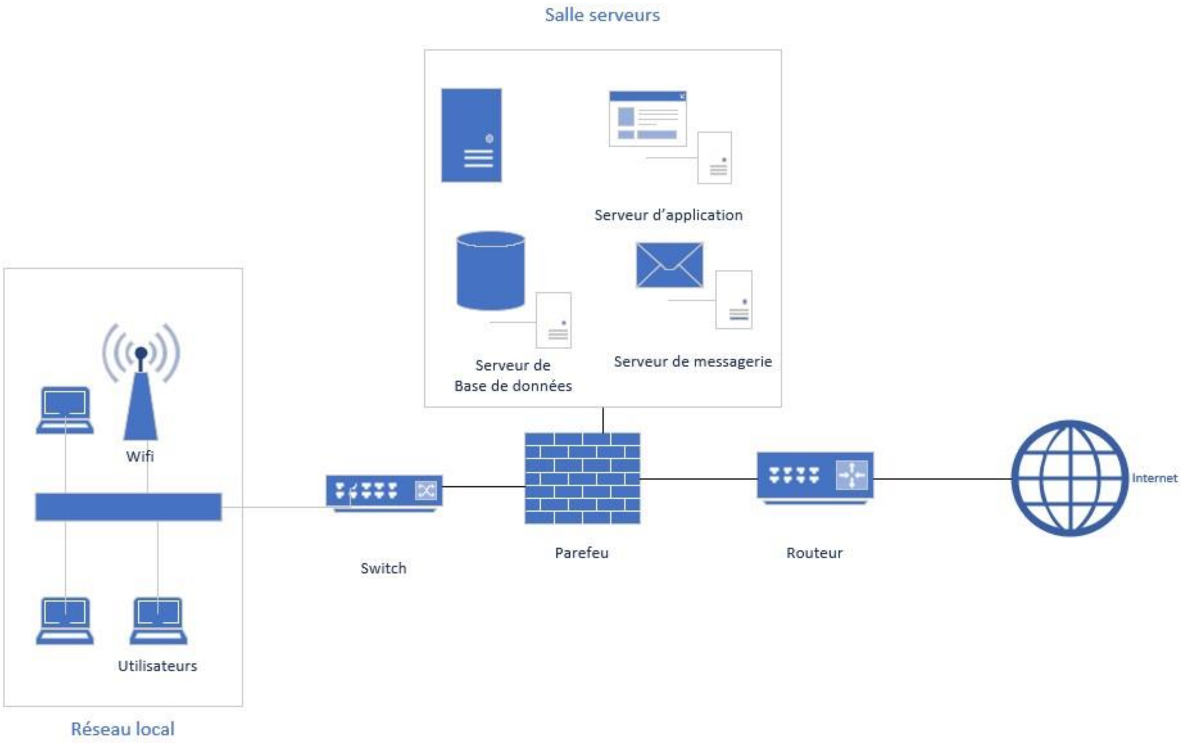


figure1: Existing architecture IP-TELRA

# Study of the means of processing information

## Material resources

The company has within it a large number of computers, a dedicated server, printers, inverters, stabilizers and tools available for the network (Switch, router). The main IT tools of the structure are listed in the following table:

Picture1: IP-TELRA hardware means

| Equipment | Number | Model | Use |
|---|---|---|---|
| **Router** | 01 | Cisco 1921 | Manage network and connections |
| **internet-modem** | 01 | Camtel Huawei Hg8245 Modem | Internet access |
| **firewall** | 01 | Cisco ASA5505 | Control incoming and outgoing network traffic |
| **Waiter** | 04 | DELL PowerEdge T430 tower server | Storage of data and services |
| **Switch** | 02 | Cisco Catalyst 2960 | Filtering and connectivity of workstations |
| **Desktop** | 08 | DELL Optiplex 790 core i5 8gb ram | Allows employees to do their jobs in-house |
| **Laptop** | 06 | Dell E5450 i5-5300U -8GB ram | Allows employees to perform their work on the go |
| **Wi-Fi hotspot** | 03 | TP LinkTL-WR740N | Give wifi access to users |
| **Photocopier** | 01 | Canon IR Advance C5535i | Allows you to perform printing and photocopying tasks |

## Software resources

The company also has a set of software means in performing these functions. The software mainly used within the structure is listed in the table below:

Picture2: Medium IP-TELRA software

| Software | Version | Usefulness |
|---|---|---|
| **System Software** | | |
| **Windows 10** | 10 21H2 Professional (October 2021) | Operating system for user workstations |
| **Ubuntu** | 20.04<br>April 23, 2020 | Server system for backups and replications |
| **windows server 2016** | 1607 (10.0.14393.2363) (July 10, 2018) | For the management of workstations, configurations and support for certain services and resources. |
| **Application Software** | | |
| **Microsoft office 2019** | 2206 (16.0.15330.20246) / July 12, 2022 | For any entries, word processing, spreadsheet, note, etc. |
| **Microsoft 365** | Version 2208 (Build 15601.20148) | For any entries, word processing, spreadsheet, note, etc. |
| **SQLServer 2012** | 11.0.2100.60<br>04/23/2021 | For database management |
| **VSCode** | 2019 v16.11.6 | For the design of sites and applications |
| **Windows Teams** | 12.0 (7/28/2021) 6Sep 2022 | For online meetings and exchanges |
| **android-studio-2020** | 2021.2.1 (Chipmunk)/ May 9, 2022 | For the design of Android applications |
| **Kaspersky Total Security Antivirus** | 21.3. 10.391<br>Jul 18, 2022 | For the protection of workstations against computer viruses |
| **HTML, CSS, JavaScript, JAVA, LARAVEL, C++** | / | As a programming language. |

### Human resources

The IT department of the general management of the IP-TELRA Group is made up of a qualified, capable and dynamic IT specialist capable of assuming the missions assigned to it with so much dedication.

The aim of the critic of the existing is to identify the strengths and weaknesses of the current system; In this case, the analyst proceeds to an objective critique of the current system.

## Strengths of the existing system

In this section we highlight the strengths in the organization, architecture and security of the IP-TELRA structure.

**From the average human point of view:**The general management of the IP-TELRA Group is full of qualified and dynamic personnel to perform most of these functions;

**From the point of the information system:**It is useful to specify that it is encouraging to note that within the general management of the IP-TELRA Group, the workstations are operational and occupied by personnel capable of carrying out the work in the position to which they are assigned.

**From a technical point of view:**we note the presence of a replication and backup server to guarantee the availability of data in the event of a disaster as well as an energy continuity system in the event of a power failure.

**From a maintenance point of view:**the system maintenance team provides regular and corrective updates in terms of security for all operating systems and software.

**From an access control point of view:**the administrator adapts the USB drive blocking policy and the filtering of access from and to the Internet network to avoid the risk of spreading viruses.

**From a security point of view:**Each workstation has an up-to-date Kaspersky antivirus. The architecture is protected by a Cisco physical firewall located at the entrance to the network, it filters traffic coming from outside the network in order to detect possible threats.

## The weak points of the existing system

In this section we raise security deficiencies in IP-TELRA's architecture, solutions and security policy.

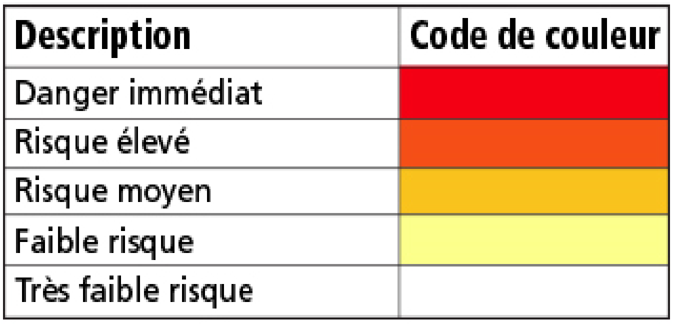
The first security breach here that is of particular interest to us is the lack of a robust security system to deal with potential attacks from hackers. They are limited here to just a fairly minimal and basic security which is largely insufficient in terms of the importance of the data to be secured.

We also note other security breaches listed here by increasing degree of criticality, namely:

Picture3: Weak point of the existing system

| Danger | Risk | Criticality threshold |
|---|---|---|
| **The slowness in the transmission of data within the hierarchy of the company.** | Slowness in transmissions and decision-making in the event of a claim. | 🟨 |
| **Absence of a procedural guide.** | Poor recovery of activities in the event of a disaster. Slowness in performing tasks. | 🟨 |
| **Absence of a security policy.** | Undetected threat, no risk assessment and no disaster recovery plan. | 🟧 |
| **Security audit not carried out within the structure since its creation** | Determination of weak points in order to be able to remedy them, non-compliance with standards | 🟧 |
| **The insufficiency of computer scientists for the multiple tasks that are carried out there.** | Overload in work which leads to lower productivity. | 🟧 |
| **Absence of a policy on strengthening passwords.** | Password theft, identity theft, information theft | 🟧 |

| | | |
|---|---|---|
| **The absence of a monitoring system.** | Business interruption due to hardware or software failure | 🟥 |
| **The absence of a network intrusion detection system and a means of anticipating threats related to data access via the Internet.** | Hacker attacks, loss of information and sensitive data, financial loss. | 🟥 |
| **The absence of a team dedicated to monitoring, monitoring security and investigating security incidents.** | Network hacking, malicious agent intrusions into the network, information loss and financial loss. | 🟥 |

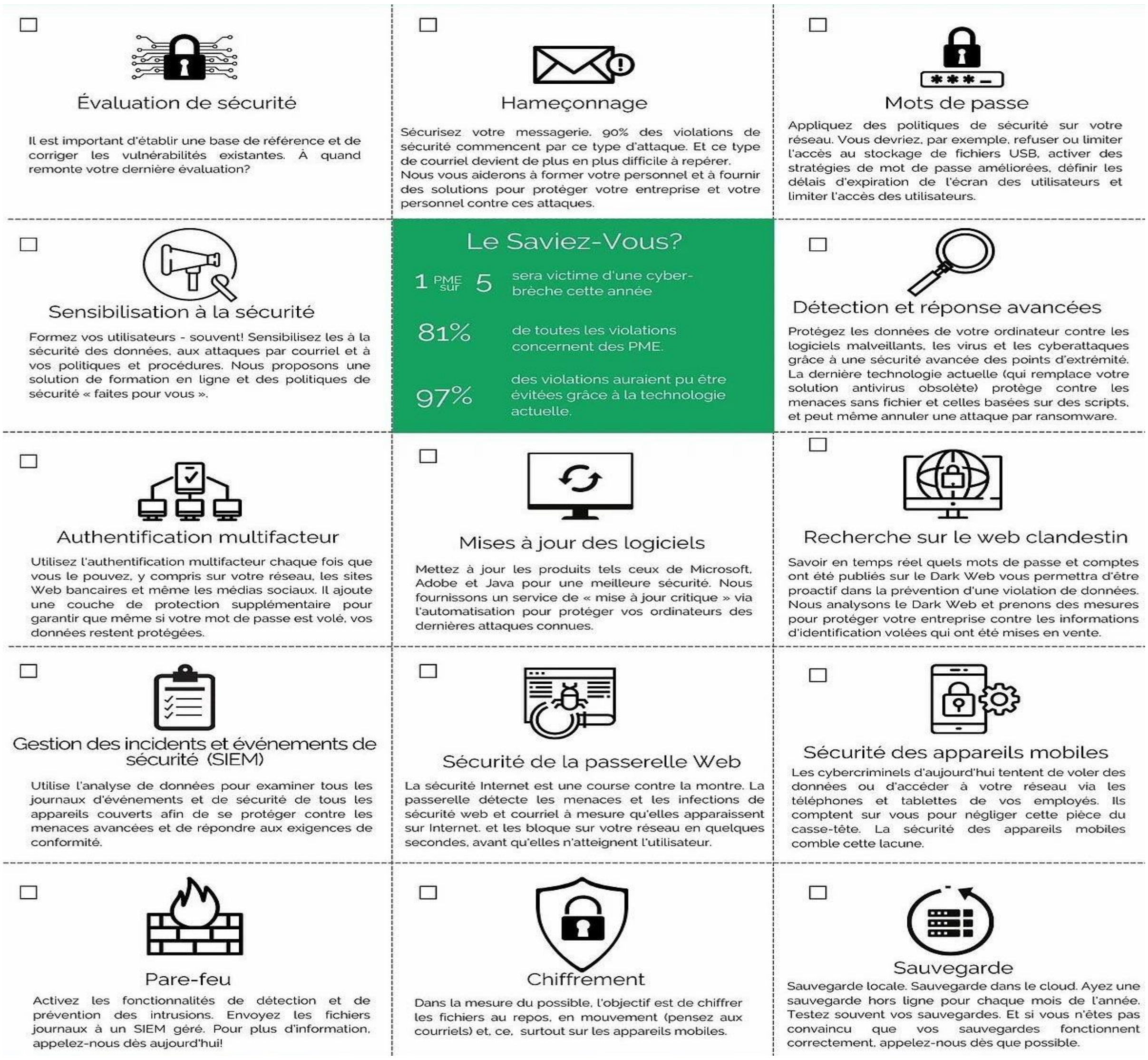


| Description | Code de couleur |
|---|---|
| Danger immédiat | 🟥 |
| Risque élevé | 🟧 |
| Risque moyen | 🟨 |
| Faible risque | 🟨 |
| Très faible risque | |

figure2: Risk color code[9]

## Some suggested solutions

In response to all the threats observed within the structure, we propose a set of solutions[8]



□ Évaluation de sécurité

Il est important d'établir une base de référence et de corriger les vulnérabilités existantes. À quand remonte votre dernière évaluation?

□ Hameçonnage

Sécurisez votre messagerie. 90% des violations de sécurité commencent par ce type d'attaque. Et ce type de courriel devient de plus en plus difficile à repérer. Nous vous aiderons à former votre personnel et à fournir des solutions pour protéger votre entreprise et votre personnel contre ces attaques.

□ Mots de passe

Appliquez des politiques de sécurité sur votre réseau. Vous devriez, par exemple, refuser ou limiter l'accès au stockage de fichiers USB, activer des stratégies de mot de passe améliorées, définir les délais d'expiration de l'écran des utilisateurs et limiter l'accès des utilisateurs.

□ Sensibilisation à la sécurité

Formez vos utilisateurs - souvent! Sensibilisez les à la sécurité des données, aux attaques par courriel et à vos politiques et procédures. Nous proposons une solution de formation en ligne et des politiques de sécurité « faites pour vous ».

Le Saviez-Vous?

1 PME sur 5 sera victime d'une cyber-brèche cette année

81% de toutes les violations concernent des PME.

97% des violations auraient pu être évitées grâce à la technologie actuelle.

□ Détection et réponse avancées

Protégez les données de votre ordinateur contre les logiciels malveillants, les virus et les cyberattaques grâce à une sécurité avancée des points d'extrémité. La dernière technologie actuelle (qui remplace votre solution antivirus obsolète) protège contre les menaces sans fichier et celles basées sur des scripts, et peut même annuler une attaque par ransomware.

□ Authentification multifacteur

Utilisez l'authentification multifacteur chaque fois que vous le pouvez, y compris sur votre réseau, les sites Web bancaires et même les médias sociaux. Il ajoute une couche de protection supplémentaire pour garantir que même si votre mot de passe est volé, vos données restent protégées.

□ Mises à jour des logiciels

Mettez à jour les produits tels ceux de Microsoft, Adobe et Java pour une meilleure sécurité. Nous fournissons un service de « mise à jour critique » via l'automatisation pour protéger vos ordinateurs des dernières attaques connues.

□ Recherche sur le web clandestin

Savoir en temps réel quels mots de passe et comptes ont été publiés sur le Dark Web vous permettra d'être proactif dans la prévention d'une violation de données. Nous analysons le Dark Web et prenons des mesures pour protéger votre entreprise contre les informations d'identification volées qui ont été mises en vente.

□ Gestion des incidents et événements de sécurité (SIEM)

Utilise l'analyse de données pour examiner tous les journaux d'événements et de sécurité de tous les appareils couverts afin de se protéger contre les menaces avancées et de répondre aux exigences de conformité.

□ Sécurité de la passerelle Web

La sécurité Internet est une course contre la montre. La passerelle détecte les menaces et les infections de sécurité web et courriel à mesure qu'elles apparaissent sur Internet. et les bloque sur votre réseau en quelques secondes, avant qu'elles n'atteignent l'utilisateur.

□ Sécurité des appareils mobiles

Les cybercriminels d'aujourd'hui tentent de voler des données ou d'accéder à votre réseau via les téléphones et tablettes de vos employés. Ils comptent sur vous pour négliger cette pièce du casse-tête. La sécurité des appareils mobiles comble cette lacune.

□ Pare-feu

Activez les fonctionnalités de détection et de prévention des intrusions. Envoyez les fichiers journaux à un SIEM géré. Pour plus d'information, appelez-nous dès aujourd'hui!

□ Chiffrement

Dans la mesure du possible, l'objectif est de chiffrer les fichiers au repos, en mouvement (pensez aux courriels) et, ce, surtout sur les appareils mobiles.

□ Sauvegarde

Sauvegarde locale. Sauvegarde dans le cloud. Ayez une sauvegarde hors ligne pour chaque mois de l'année. Testez souvent vos sauvegardes. Et si vous n'êtes pas convaincu que vos sauvegardes fonctionnent correctement, appelez-nous dès que possible.

figure3: Computer system security solution

# Material and method

The functional analysis of an IT project is a step that is necessary and essential to carry it out. It makes it possible to design a system for which all the options will be perfectly designed, oriented towards maximum customer satisfaction. It is with this in mind that before starting this project, we will comprehensively analyze its environment in order to understand the issues and potential constraints.

# Project display

With the evolution of communication techniques, information systems and computer networks are now increasingly open to the outside world, particularly with the Internet. This openness makes life easier for humans by offering them various services, and connects hundreds of millions of machines to the Internet all over the world. However, this interconnection of machines also allows malicious users to use these resources and take advantage of its vulnerabilities for abusive purposes, for example: making a web service offline.

Security nowadays is a problem of paramount importance, it has become a major problem in the management of corporate networks as well as for individuals. Different mechanisms have been put in place to deal with these security problems, such as antivirus, firewalls, encryption, but these mechanisms have limits in the face of the rapid development of hacking techniques. To avoid these limits, the use of intrusion detection systems is essential.

Intrusion detection systems are designed for continuous monitoring and discovery of security policy violations, thus identifying any unauthorized activity in a network. Honeypots, on the other hand, are used to deceive hackers in order to gather information on the modes of action in the network. The distributed system allows the sharing of information on attacks in real time in the different sites so that measures are taken to counter this.

# Problem

IP-TELRA being a young company also offering online storage services with some of these partners, it contains a large amount of mostly confidential data, the hacking of which could prove fatal for the company. Until now, no study has yet been carried out to guarantee administrators of knowing exactly the types of data (offensive or not) that pass through network installations as well as the types of activities carried out by users there. are connected. You shouldn't always wait for tragedy to happen before taking corrective action. Security must be as preventive as possible in order to avoid possible threats. Zero risk does not exist in security, we can still get closer to it by setting up a good security system. It is therefore necessary to offer the network an environment for controlling the types of activities (offensive or not) that take place there. Also, it is important to have a space for studying attacks that would target network equipment. This will allow network administrators to track new vulnerabilities exploited by hackers as well as new hacking tools.

# Methodology and technical choices

Our proposal requires the use of several tools including intrusion detection systems (IDS) and honeypots. We present here our work methodology and the technical choices made.

## Methodology of work

This work focuses on large area networks in general and IP-TELRA in particular. In this network, we distinguish IP-TELRA client networks and private infrastructures (service servers and network equipment) from the network itself. Thus, it is necessary to proceed to the analysis of the data on each site of the network. For this, we study intrusion detection systems in order to choose the most appropriate system according to our objectives, in particular communication between autonomous instances. This choice allows us to train our distributed environment across the network. Next, we propose the space for studying the strategies, tools and commands used by hackers, with a view to each time adapting the security policy of the entire network to new threat trends. It is precisely a network of honeypots. We therefore analyze the types of honeypots as well as the deployment technologies of honeynet (honeypot network) with the aim of providing the best possible environment. The final stage is devoted to the various tests in order to validate our various proposals.

## Choice of intrusion detection system

There are different intrusion detection systems with different characteristics which we discussed in Chapter 3. For the monitoring of each IP-TELRA customer site, we use a network intrusion detection system. Network IDS are more appropriate in that they not only do not require touching machines already in production but also allow monitoring of a whole set of machines from a single point. It is therefore a lower cost technology requiring fewer resources. In addition, they do not overload the network and allow easier management of maintenance. In the literature, the most advanced tools that can perform this function are Snort, Suricata and Bro. Our approach is based on a distributed architecture with fully autonomous agents. In this architecture, we establish communications between the different agents. So the NIDS should allow us to implement that. Thus, Bro emerged as the tool of choice. Compared to these direct competitors, Bro is definitely more technologically advanced. It gives the possibility of personalizing it according to the desired objectives. It is flexible with a built-in language that can be used to create all sorts of network tools.

## Spots done by Bro (Zeek)

Zeek performs two key tasks that benefit security organizations:

1) Converts network traffic data into higher-level events;

2) Provides a script interpreter, a robust programming language that is used to interact with events and understand what those events mean in terms of network security.

In other words, Zeek captures metadata about activity on a network and then provides a programming language to understand when that activity shows malicious or suspicious indications.

## Bro compared to conventional IDS

When Bro (Zeek) monitors a flow of traffic, he produces logs that record everything he understands about network activity. This understanding includes connection records, volume of packets sent and received, attributes of TCP sessions, and other metadata useful for analyzing network behavior and understanding the context of that behavior.

What is considered suspicious network behavior in one organization, perhaps routine in another? This is why the Bro (Zeek) programming language is so advantageous; it can be used to customize the interpretation of metadata to an organization's specific needs.

Bro (Zeek) provides a way to perform the same kinds of checks for traffic attributes, but with the added value of a programming interface. This means that Bro(Zeek) can be used to calculate numerical statistics and regular expression pattern matches. It can also create complex logical conditions using AND, OR, and NOT operators, which allow users to customize the analysis to suit their environment.

## Bro Deployment Specification

The deployment of Bro strongly depends on the security policy adopted by the organization. Placed behind an external firewall, this configuration allows Bro to only receive packets filtered according to the rules defined in the firewall. This results in fewer notifications. However, some organizations prefer to install it without this firewall in order to be notified of all attempted attacks. Another option is to place it behind the internal firewall allowing it to detect internal machines infected with viruses and worms.

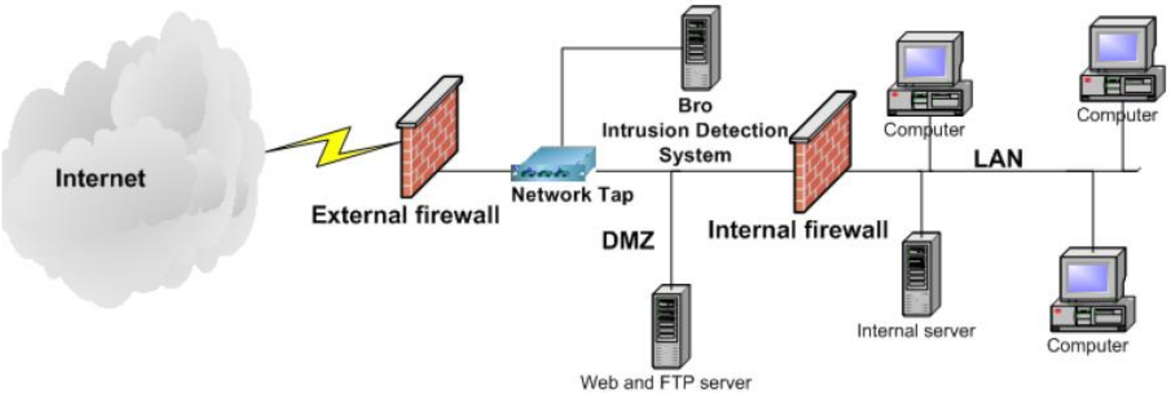


figure4: Typical location of a sensor and the Bro system

Bro does not require a specialized machine, and can work well on a cheap machine. However the system must monitor all packets entering and leaving the site. So depending on the network traffic, it may be necessary to use a fairly robust machine.

The following table gives a summary of the requirements required for the deployment of Bro according to the characteristics of the network of the host.

# Results :

We were able to set up an intrusion detection and prevention system using the bro intrusion prevention and detection system coupled with a honeypot network, thus reducing the company's level of vulnerability. Our main challenges encountered were in terms of the complexity of implementation and also in the acquisition of sophisticated hardware to be able to support the solution.

# Conclusion

Monitoring the data passing through a network not only protects against threats, but also avoids being a staging area for attacks. In this project, the aim of our work was to set up an intrusion detection and prevention system using sensors distributed in a network in order to increase the level of security of the company IP-TELRA , we proposed in a general way, a distributed architecture of detection and prevention of intrusions based on autonomous agents; then we integrated it into the architecture of the IP-TELRA network. To this end, we used the NIDS Bro, which we deployed as a network analyzer at each site. Each instance of the architecture shares events with the other instances. To achieve this, we have developed two scripts in Bro language: sender.bro and receiver.bro. These scripts therefore make it possible to establish communication between the different agents as well as the reactions to adopt when these events occur. Additionally, we have proposed a honeypot network for studying hacking attacks and tools. The information collected in this space will track vulnerabilities that hackers could exploit in the IP-TELRA network. As a result, administrators will need to adopt the necessary response to reduce these vulnerabilities. we have proposed a network of honeypots intended for the study of attacks and hacking tools. The information collected in this space will track vulnerabilities that hackers could exploit in the IP-TELRA network. As a result, administrators will need to adopt the necessary response to reduce these vulnerabilities. we have proposed a network of honeypots intended for the study of attacks and hacking tools. The information collected in this space will track vulnerabilities that hackers could exploit in the IP-TELRA network. As a result, administrators will need to adopt the necessary response to reduce these vulnerabilities.

In order to be able to benefit from the advantages of centralized management, we propose as a perspective for this work, the implementation of mechanisms for collecting events or alerts towards a central management entity. We would then have an architecture coming from a combination of distributed architecture based on completely autonomous agents and centralized distributed architecture. Also, with the possibilities offered by Bro, it would be useful to instrument, i.e. rewrite, using Broccoli, the applications (SSH, HTTPS, etc.) running on the honeynet servers so that they send to Bro the data they actually received. This will allow for example to track encrypted connections that it is not possible to analyze at the network level.